

CLAIMS

What is claimed is:

1. A computerized method comprising:
 - monitoring a peer-to-peer network for suspicious activity based on patterns of activity; and
 - performing an action associated with a particular pattern when the particular pattern is detected in the peer-to-peer network.
2. The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:
 - evaluating network traffic among peers in the peer-to-peer network.
3. The computerized method of claim 1, wherein monitoring a peer-to-peer network comprises:
 - evaluating a change in shared data on a peer in the peer-to-peer network.
4. The computerized method of claim 1, wherein a pattern of activity is defined in terms of a threshold value of network traffic in the peer-to-peer network.
5. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that uses a specific protocol.
6. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network that accesses shared data on a peer.
7. The computerized method of claim 1, wherein a pattern of activity is defined in terms of network traffic in the peer-to-peer network having a foreign address.

1002844-122101
101221-218200

- 1 8. The computerized method of claim 1, wherein a pattern of activity is defined in
2 terms of a configuration of shared data on a peer.

- 1 9. The computerized method of claim 1, wherein the action comprises logging
2 information about the particular pattern.

- 1 10. The computerized method of claim 1, wherein the action comprises sending an
2 alert about the particular pattern.

- 1 11. The computerized method of claim 1, wherein the patterns of activity are local to a
2 peer in the peer-to-peer network.

- 1 12. The computerized method of claim 1, wherein the patterns of activity are global to
2 the peer-to-peer network.

- 1 13. The computerized method of claim 1 further comprising:
2 obtaining a set of rules specifying the patterns of activity and associated actions.

- 1 14. The computerized method of claim 13 further comprising:
2 refreshing the set of rules when the set of rules changes.

- 1 15. A computer-readable medium having executable instructions to cause a processor
2 to perform a method comprising:
3 monitoring a peer-to-peer network for suspicious activity based on patterns of
4 activity; and
5 performing an action associated with a particular pattern when the particular
6 pattern is detected in the peer-to-peer network.

1 16. The computer-readable medium of claim 15, wherein the method further
2 comprises:
3 evaluating network traffic among peers in the peer-to-peer network when
4 monitoring the peer-to-peer network.

1 17. The computer-readable medium of claim 15, wherein the method further
2 comprises:
3 evaluating a change in shared data on a peer in the peer-to-peer network when
4 monitoring the peer-to-peer network.

1 18. The computer-readable medium of claim 15, wherein a pattern of activity is
2 defined in terms of a threshold value of network traffic in the peer-to-peer network.

1 19. The computer-readable medium of claim 15, wherein a pattern of activity is
2 defined in terms of network traffic in the peer-to-peer network that uses a specific
3 protocol.

1 20. The computer-readable medium of claim 15, wherein a pattern of activity is
2 defined in terms of network traffic in the peer-to-peer network that accesses shared data on
3 a peer.

1 21. The computer-readable medium of claim 15, wherein a pattern of activity is
2 defined in terms of network traffic in the peer-to-peer network having a foreign address.

1 22. The computer-readable medium of claim 15, wherein a pattern of activity is
2 defined in terms of a configuration of shared data on a peer.

- 1 23. The computer-readable medium of claim 15, wherein the action comprises logging
2 information about the particular pattern.
- 1 24. The computer-readable medium of claim 15, wherein the action comprises sending
2 an alert about the particular pattern.
- 1 25. The computer-readable medium of claim 15, wherein the patterns of activity are
2 local to a peer in the peer-to-peer network.
- 1 26. The computer-readable medium of claim 15, wherein the patterns of activity are
2 global to the peer-to-peer network.
- 1 27. The computer-readable medium of claim 15, wherein the method further
2 comprises:
3 obtaining a set of rules specifying the patterns of activity and associated actions.
- 1 28. The computer-readable medium of claim 27, wherein the method further
2 comprises:
3 refreshing the set of rules when the set of rules changes.
- 1 29. A system comprising:
2 a processor coupled to a memory through a bus;
3 a network interface coupled to the processor through the bus and further operable
4 to selectively couple to a peer-to-peer network; and
5 a peer-to-peer security process executed by the processor from the memory to
6 cause the processor to monitor the peer-to-peer network for suspicious activity based on
7 patterns of activity, and to perform an action associated with a particular pattern when the
8 particular pattern is detected in the peer-to-peer network.

1 30. The system of claim 29, wherein peer-to-peer security process further causes the
2 processor to evaluate network traffic between the peers in the peer-to-peer network when
3 monitoring the peer-to-peer network.

1 31. The system of claim 29 further comprising a computer-readable medium coupled
2 to the processor through the bus, and wherein the peer-to-peer security process further
3 causes the processor to evaluate a change in shared data on the computer-readable medium
4 when monitoring the peer-to-peer network.

1 32. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to monitor the peer-to-peer network for a pattern of activity defined in terms
3 of a threshold value of network traffic in the peer-to-peer network.

1 33. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to monitor the peer-to-peer network for a pattern of activity defined in terms
3 of network traffic in the peer-to-peer network that uses a specific protocol.

1 34. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to monitor the peer-to-peer network for a pattern of activity defined in terms
3 of network traffic that accesses shared data on a peer.

1 35. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to monitor the peer-to-peer network for a pattern of activity defined in terms
3 of network traffic having a foreign address.

1 36. The system of claim 29 further comprising a computer-readable medium coupled
2 to the processor through the bus, and wherein the peer-to-peer security process further

3 causes the processor to monitor the peer-to-peer network for a pattern of activity defined in
4 terms of a configuration of shared data on the computer-readable medium.

1 37. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to log information about the particular pattern when performing the action
3 associated with the particular pattern.

1 38. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to send an alert about the particular pattern when performing the action
3 associated with the particular pattern.

1 39. The system of claim 29, wherein the system is a peer in the peer-to-peer network
2 and the patterns of activity are local to the system.

1 40. The system of claim 29, wherein the system is a server in the peer-to-peer network
2 and the patterns of activity are global to the peer-to-peer network.

1 41. The system of claim 40, wherein the system is a border firewall.

1 42. The system of claim 40, wherein the system is a domain name server.

1 43. The system of claim 29, wherein the peer-to-peer security process further causes
2 the processor to obtain a set of rules specifying the patterns of activity and associated
3 actions.

1 44. The system of claim 43, wherein the peer-to-peer security process further causes
2 the processor to refresh the set of rules when the set of rules changes.